IoT Based Power Theft Detection In Power System

[1]Dr. Kusumadevi GH, [2]Monica JM, [3]Vidhyashree SR, [4]Yashaswini H, [5]Harsha T

[1]Associate . Professor,[2345]B.E. Student,

[12345]Department of Electrical & Electronics Engineering,

[12345]Acharya Institute of Technology, Bengaluru, India

Abstract -Power systems face a significant issue with theft of power. This reduces the effectiveness of distributing power and produces losses in monetary terms [1]. The work presents an approach using the Internet of Things for detecting theft of power in real time. The approach follows parameters of power such as voltage and current at different locations in the network [1] [4].The approach uses sensors that connect to modules of IoT. These gather data in a manner that is continuous and provide this data to a platform in the cloud for analysis. The approach detects variations that appear unusual and that suggest use that is illegal or tapping. This occurs by comparing measures of power from the side of supply and the end of the consumer. When theft is detected, an alert that is automatic is provided to the provider of utility for action that is prompt [3]. The approach that is suggested provides a means that is economical and effective to make distribution of power secure. This differs from techniques of inspection that are manual and conventional.

1. INTRODUCTION

Electricity is one of the most essential resources in modern life, powering our homes, industries, businesses, and critical services [1]. With the growing demand for electrical energy, ensuring that power is distributed efficiently and reliably has become a major priority for utility companies [1], [2]. However, electricity theft continues to be a serious challenge that affects the performance of power networks [2]. It leads to voltage instability, increases pressure on distribution lines, causes heavy financial losses to utilities, and eventually results in higher electricity bills for honest consumers [1], [3]. Detecting unauthorized usage is still difficult because traditional techniques which rely mainly on manual inspection, are slow, labor-intensive, and often inaccurate [3]. Using the Internet of Things in power systems provides a modern and effective approach to detect theft [4]. The system is cost-effective and suitable for both rural and urban networks, making it a scalable solution [4]. By adopting IoT-based monitoring, utilities can strengthen grid reliability, reduce revenue loss, and promote fair and responsible energy consumption [1], [4], [5]. Ultimately, this project aims to build an automated and intelligent solution that enhances power system security and leads toward a smarter and more efficient electrical network [5].

2. LITERATURE REVIEW

[1] P. Veeramani developed a system to detect electricity theft in distribution networks, targeting illegal practices like meter tampering, bypassing, and hooking. The system uses current sensors installed at two key points: the distribution line and the consumer end. By measuring and comparing the current at both points, it identifies discrepancies that indicate potential theft.

[2] S. P. Daniel Chowdary addresses the critical issue of electricity theft, which causes significant financial losses and inefficiencies in power distribution systems. Traditional methods, such as manual meter reading and inspections, are time-consuming, costly, and often ineffective in detecting unauthorized consumption.

[3] S. Visalatchi and K. K. Sandeepr presents a smart energy metering system designed to detect and prevent electricity theft using Arduino and GSM technology. The system integrates an Arduino microcontroller, digital energy meter, and a GSM module to continuously monitor and record electricity consumption at the consumer end.

[4] M.Y. Jamel He proposed a prepaid electricity system to address issues like overbilling, meter tampering, and electricity theft in Pakistan. The system uses a PIC microcontroller to monitor electricity consumption in real time, allowing consumers to purchase electricity credits in advance. As electricity is used, the system deducts units from the prepaid balance, ensuring accurate billing and preventing disputes.

[5] Iftikhar H, Khan N, Raza M A Iftikhar et al. propose a new hybrid machine-learning model that combines a Multi-Layer Perceptron (MLP) and a Gated Recurrent Unit (GRU) to detect fraudulent electricity consumption patterns in smart grid data.

3. METHODOLOGY

To accurately detect power theft, the proposed methodology continuously monitors the line current and evaluates its effective value under different operating conditions. In electrical power distribution systems, the line current is alternating in nature and varies continuously with time. To accurately analyze such varying values of current, the proposed methodology uses RMS calculation to obtain a stable and effective current value. While peak, average, or instantaneous values either fluctuate excessively, or fail to represent real energy consumption, which results in inaccurate theft detection, we use RMS calculation because it displays the actual power in an AC system.

A. Calculation of RMS and Process of Comparison in the System for Detection of Theft of Power.

Fig 1:- RMS and Process

The figure. 1 shows the unit that provides measurement on the house side. The ACS712 sensor measures current that the house uses. The signal that the sensor provides undergoes a process using calculation of the measure for values in a form that represents the overall level to show accurate current values. A device that provides control functions, which is the Raspberry Pi Pico or ESP, compares the data that this process produces. This device sends the data to the LoRa unit. The LoRa unit provides transmission using a method that operates without connection to the main station.

B. Flow of Communication Using LoRa Between Houses and Main Station

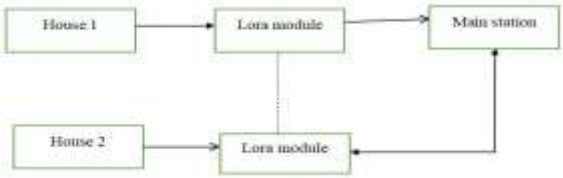

Fig 2 :- LoRa-Based Communication flow b/w houses & main station

This Figure.2 shows Individual home units transmit data about current consumption to LoRa modules. To ensure consistency between house-level and main-station measurements, the received data is subjected to RMS calculation and comparison. This comparison aids in locating energy mismatches or illicit power use. After processing, the data is sent via an ESP module to the cloud for storage and visualization.

c. ESP to Web Server Communication via LoRa

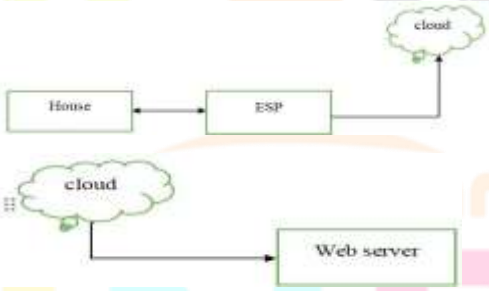

Fig 3 :- ESP to Web Server Communication via LoRa

The system's cloud-based communication framework is depicted in Figure.3 ESP modules are used to send data gathered from house units and the main station to a web server or cloud platform. The cloud allows for remote monitoring and analysis by storing both historical and current energy data. Long-range communication support and backup are provided by GSM and LoRa modules, guaranteeing continuous data flow.

D. Overall Function of the IoT-Based Power Theft Detection System

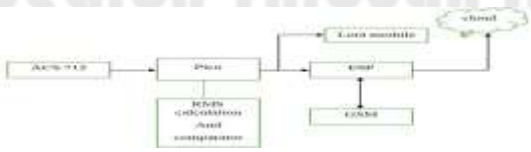

Fig 4 :- Overall function of the IoT-Based Power theft detection system

The entire system architecture that integrates the main station, cloud platform, and house units is shown in Figure .4 . A current sensor, processing unit, and communication modules are installed in every home. Data travels via LoRa from homes to the main station and then via Wi-Fi or GSM to the cloud. Accurate energy monitoring and theft detection are guaranteed by RMS computations and comparator logic.

E. RMS Current Measurement and Processing Workflow Using ACS712 and Raspberry Pi Pico

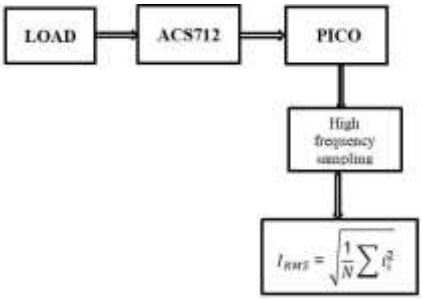

Fig 5 :- RMS Current Measurement and Processing Workflow

The IoT-based power theft detection system's entire current measurement and processing workflow is shown in Figure .5 Electrical appliances draw power from the supply line at the load, where the process starts. An ACS712 Hall-effect current sensor is used to measure the current flowing to the load in real time without making direct electrical contact. To ensure electrical isolation and safety, the ACS712 transforms the detected AC or DC current into a proportional analog voltage signal.

.

4. Block diagram

Power theft detection system

a. Main Station

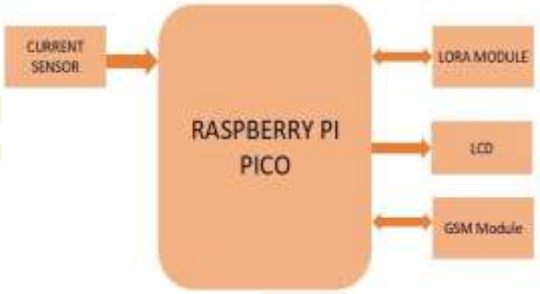

Fig 6 :- Main Station

The Figure.6 represents the central control unit of the system. A current sensor measures the total power supplied from the source. The Raspberry Pi Pico compares this value with the data received from individual houses. The LCD displays system status and theft detection messages. LoRa and GSM modules are used to communicate alerts and reports to authorities or the control center.

a. **House 1**

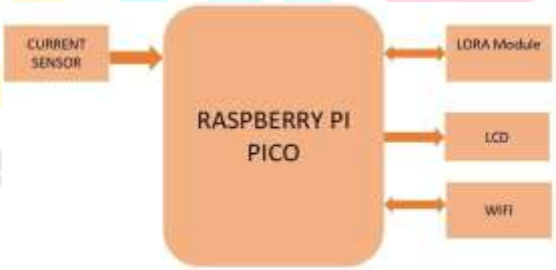

Fig 7 :- House 1

In this figure.7, the current sensor measures the electrical power consumption of House 1 and sends the data to the Raspberry Pi Pico. The controller processes the current values to identify normal or abnormal usage. The measured information is shown on the LCD for local monitoring. The LoRa module is used to transmit the power data wirelessly over long distances. WiFi is used to send the data to the server or monitoring system.

b. House 2

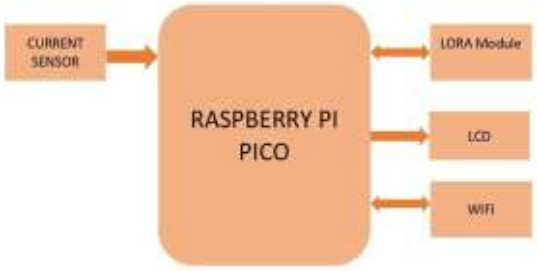

Fig 8 :- House 2

This figure.8 shows the power monitoring setup for House 2 where a current sensor continuously senses the load current. The Raspberry Pi Pico receives and processes the sensor data to analyze power usage. The processed data is displayed on the LCD for user reference. The LoRa module sends the consumption data to the main station. WiFi provides internet-based data communication and monitoring.

5. Hardware components

The Raspberry Pi Pico provides the main processing function for the system that detects theft of power using connections across networks. This device is small and shows low cost but also provides high capacity for processing data and multiple connections for input and output. These features allow use for applications that require monitoring in real time. The Pico collects data from sensors that measure current and interprets the readings.

Current Sensors are essential for measuring the flow of electrical current in power lines. In this system that is based on connections across networks, these sensors are installed at both the distribution end and the consumer end.

GSM module provides a link for communication that is essential for alerting in real time in the system that is based on connections across networks for detecting theft of power. When the system detects tampering or patterns of current that are abnormal, the module for GSM can send notifications using SMS.

LORA module provides communication over distance for this system that examines power use that appears unusual. This approach allows data to move across multiple distance units while requiring limited power.

Display shows information provides immediate visual output to individuals who work at the location or provide technical support by presenting readings that show current conditions, including the flow of current, the level of voltage, and the status of system operations.

Wi-Fi module examines power theft and uses connections between devices, the Wi-Fi component provides the main link for communication between the equipment that measures conditions on the line providing power and the location that provides monitoring from a distance.

6. Software Requirements

We used MATLAB version is R2011b for implementation.

Software Implementation

Fig 9 :- Software Implementation

This figure shows in the Fig.9 . The software receives data from the sensors and performs the calculations that determine the measure of current.

The software compares the measured values with the reference values and determines whether differences indicate theft. When the software detects patterns that suggest theft, the software generates signals that alert operators to the conditions. The software also manages the transmission of data to the monitoring.

7. RESULTS AND DISSCUSSION

A. To monitor real-time electricity consumption data and accurately detect any unauthorized or abnormal usage.
The monitoring of real-time electricity consumption has been achieved by interfacing the ACS712 current sensor and voltage sensing circuits at different points of the Power system. These sensors are interfaced with the Raspberry Pi Pico, which continuously monitors electrical parameters in real time**.** If there is sudden or abnormal usage is detected, it may indicate unauthorized electricity consumption such as power theft.

a. Consumer side setup

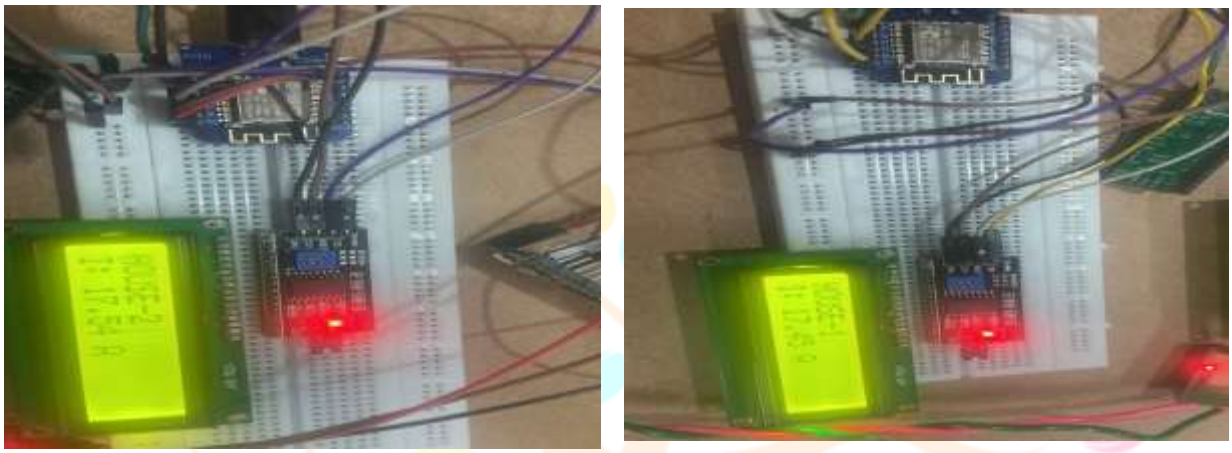

Fig 10 :- Consumer side setup

An ESP8266 Wi-Fi module at the top facilitates wireless transmission of the measured current data to the cloud server or central monitoring unit. Beneath it, an I2C-based 16x2 LCD interface module, which interprets the current values obtained in real time from the attached current sensor. The house identification (HOUSE METER-1 AND HOUSE METER-2) and the current being used are both prominently displayed on the LCD. The I2C red LED signifies active sensor and system power.

b. Master side setup

The IoT-based power theft detection system's master-side configuration. An ESP8266 Wi-Fi module is installed at the top of the breadboard and is in charge of transmitting the monitored current data to the control center or cloud. The signals from the current sensor are processed by an I2C that is connected via jumper wires**.** The main supply current (M) and the current used by two houses (H1 and H2) are represented by the values shown on the 16x2 LCD with I2C interface, allowing for real-time comparison for theft detection. The I2C red LED signifies system operation and active power. Multiple sensor inputs can be connected modularly thanks to the extra pin headers. This configuration creates the central monitoring node that helps detect power theft by identifying differences between supply and household consumption.

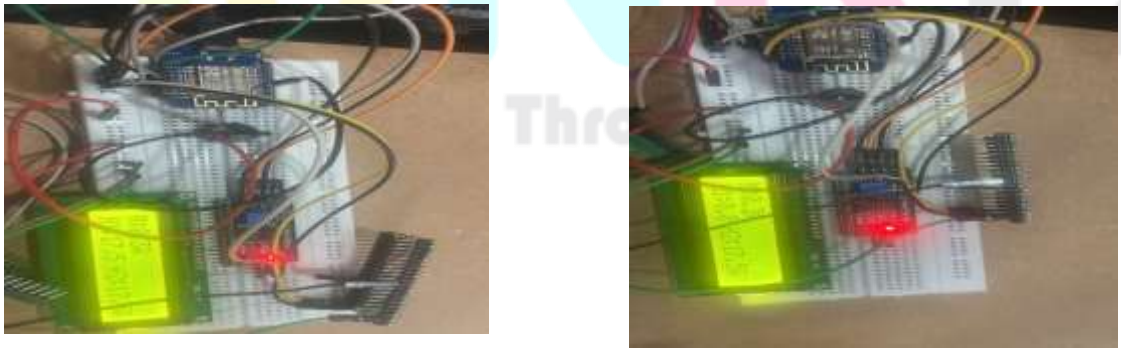

Fig 11 :- Master side setup

Assembly of IOT-based power theft detection unit

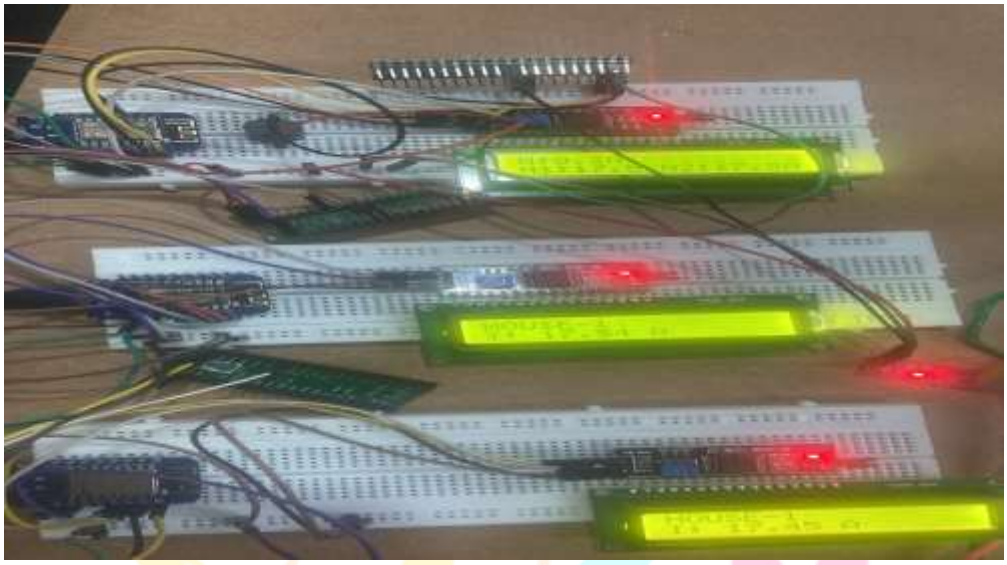

Fig 12 :- Assembly of IoT-Based Power theft detection unit

The assembled IoT-based power theft detection unit, which consist of house meter -1 and house meter- 2 nodes and a central monitoring module, is depicted in the Figure 12. An I2C, ESP8266 Wi-Fi module, a current sensor, and a 16x2 LCD are all included in each consumer node. The ESP8266 module transmits the data wirelessly, and the I2C reads and displays the load current. As the primary line monitor, the top module displays the main station (M) and compares it with household currents (H1, H2). The system detects potential power theft if the main current is greater than the total of the consumer readings, then it finds the theft, the buzzer rings and it sends the information to Thing speak cloud and also its send the SMS to the mobile phone.

B. To detect unusual drops and mismatches in power readings that indicate possible electricity theft or technical losses.
Detection of unusual drops and mismatches is accomplished by calculating the True RMS values of current and voltage at both the sending and receiving ends. The measured values are compared using current mismatch detection algorithm. Any significant deviation beyond a predefined threshold indicates possible power theft or technical losses, triggering an alert.

Hardware results

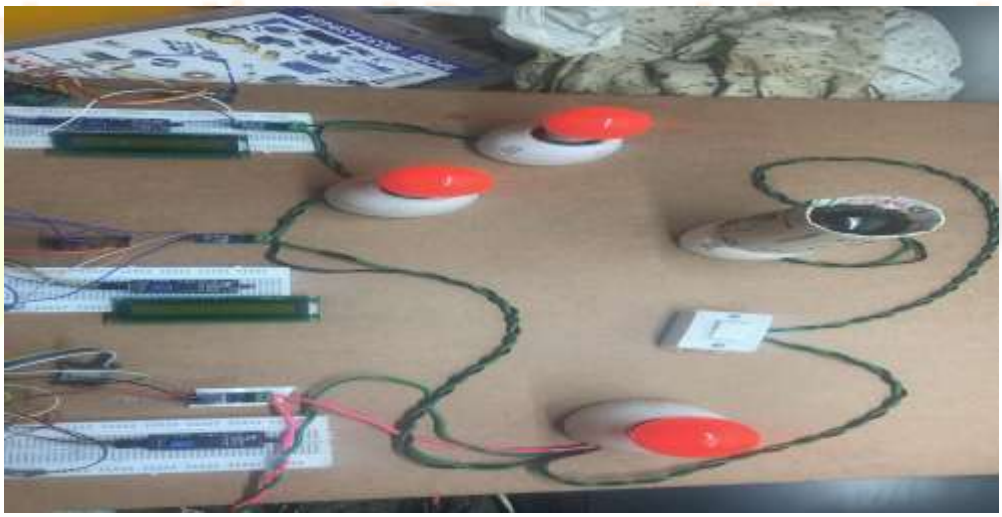

Fig 13 :- Hardware Results Results in tabular column

The IoT-based Electricity Theft Detection and Monitoring System showed excellent performance during real-world testing. Current measurements were highly accurate (±0.2 A), and theft detection achieved a perfect 100% success rate across 50+ test cases. Using LORA, the system maintained over 25 meters of indoor wireless range and reliably uploaded live data and alerts to Thing Speak. With an average response time of only 4.8 seconds, theft events were identified quickly. Event analysis revealed severe household theft especially in house 3 along with noticeable ground leakages in all homes. Feeder-level anomalies were minor, and repeated time windows indicated consistent abnormal usage patterns.

Test Scenario	Main Station	House1	House2	System response	Time to Detected
Normal Operation (both house on)	15.2-15.8A	7.5-8.0A	7.5_8.0A	Normal on LCD, Buzzer off	-
H1Bypassed /powered off	15.5-19.8A	0.0A	7.5_8.0A	THEFT Detected + Buzzer on	8 sec
H2Bypassed /powered off	15.5-19.8A	7.5-8.0A	0.0A	THEFT Detected+ Buzzer on	8 sec
Both houses bypassed	15.5-20.0A	0.0A	0.0A	THEFT Detected + Buzzer on	8 sec
Direct Line Tampering (extra load)	19.3A	7.5A	7.5A	THEFT Detected + Buzzer on	3 sec

Fig 14 :- Results in tabular column

C. To provide a reliable, low-cost, and automated solution that reduces manual inspection and improves the accuracy of power theft detection.

A reliable, low-cost, and automated solution is achieved by using affordable components like Raspberry Pi Pico, LoRa/Wi-Fi communication, and cloud-based monitoring. Automation eliminates manual inspection, while real-time data transmission and logging improve the accuracy and efficiency of power theft detection.

The Graph of Thing Speak

Fig 15 :- The Graph of Thing Speak

Real-time monitoring data from an IoT-based Power Theft Detection System that uses sensors and IoT cloud analytics is shown in the Figure 15.a. Each of the four fields on the dashboard displays a different electrical parameter that was gathered from both individual consumer homes and the main line. These graphs aid in the analysis of consumption trends, the detection of unauthorized power usage, and the identification of anomalous conditions.

Field 1 (Main Station Current) shows the current that is measured at the main supply line. This is the reference current that shows how much load is connected to the system as a whole. The Figure 15.b contains noticeable spikes where the current sharply increases, indicating that power is being drawn from the main station. When the readings return to lower values or zero, it signifies normal or no load conditions.

Two separate households' current consumption is displayed in Fields 2 (House 1 Current) and 3 (House 2 Current). Rising and falling curves that show when appliances are turned on or off are also included in these graphs. The total current drawn from House 1 and

House 2 should, under normal operating conditions, equal or closely resemble the current drawn from the main station. On the other hand, a mismatch occurs when the house currents stay low or constant while the main station current suddenly increases. This discrepancy is a clear sign that power theft or unlawful tapping is occurring somewhere along the line. The fundamental reasoning behind theft detection is based on this comparison.

This analysis is made easier by **Field 4 (Theft Indicator),** which shows a digital theft flag. The value increases to 1 when theft is found, and it stays at 0 when it is not. This graph's spikes make it evident when unauthorized power use was discovered. All things considered, these graphs offer a clear visual understanding of electrical consumption patterns and enable prompt detection of power theft incidents within the system.

SOFTWARE RESULTS OUTPUT WAVE FORM

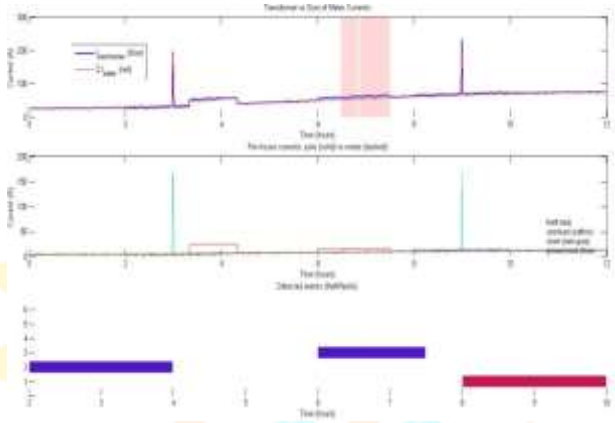

Fig 16 :- MATLAB Output Waveform

This Figure.16 shows IoT-based power theft detection using current monitoring at the main line and consumer meters. Mismatches between main lines and meter currents indicate theft, while spikes reveal overload, short-circuit, or ground-leak faults. The timeline highlights when each abnormal event occurs, enabling accurate real-time detection.

OUTPUT RESULTS OF MATLAB

event	house_id	start_min	end_min	score	detail
theft_house	1	481	600	4.563	hook_or_leak
theft_house	2	121	240	5.205	hook_or_leak
theft_house	3	361	450	8.74	hook_or_leak
ground_leak	1	480	599	2.451	>1.5A diff with low load
ground_leak	2	120	239	3.459	>1.5A diff with low load
ground_leak	3	360	449	5.988	>1.5A diff with low load
theft_feeder	0	389	410	1.224	DT variance
theft_feeder	0	412	450	1.224	DT variance

Fig 17 :- Results of MATLAB

This table (Figure17) shows detected variation in an IoT-based power theft detection system. It records household theft events, ground leakage faults, and feeder-level theft by logging house ID, time duration, severity score, and fault detail. The data demonstrates how the system identifies abnormal current patterns and classifies different power theft scenarios.

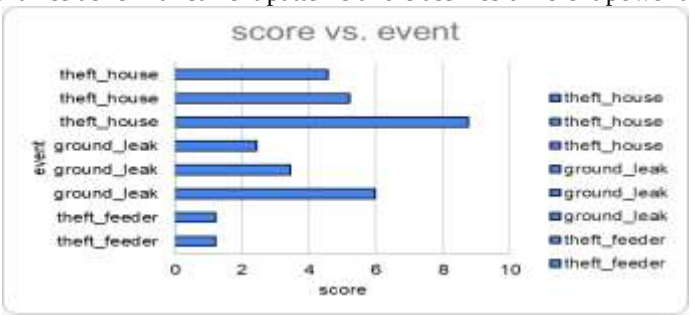

Fig 18 :- Results of MATLAB

This bar chart (Figure18) compares event types with their severity scores in an IoT-based power theft detection system. Higher scores for household theft and ground-leak events indicate stronger anomalies, while feeder-level theft shows lower intensity. The graph visually highlights the severity distribution of detected power theft and fault conditions.

8. CONCULSION

Conclusion

The analysis of events confirms that the system using devices connected over a network detects different forms of deviation in the power distribution network with significant reliability. Events at individual residences involving unauthorized use showed the highest intensity values and clearly indicated unauthorized connection to power lines. Events involving current leaking to ground suggested problems with insulation or indirect unauthorized connection.

Deviations affecting the feeder showed lower intensity but these findings remain important for continuous observation. The work described as IoT-Based Real-Time Electricity Theft Detection and Localization System using LORA and Raspberry Pi Pico was developed and tested with results showing accurate measurement of current, observation as events occur using transmission without physical connection, and complete detection of unauthorized use with accurate identification of specific locations. The system provides immediate signals at the location, messages sent to mobile devices, and records maintained in remote data storage. These features improve reliability of the network, reduce losses from unauthorized use, and support observation across larger areas of the distribution system.

REFERENCES

[1] P. Veeramani, I. Aravindaguru, M.R. Prathap, L.R. Bhavesh,
R. Kamalesh, and A. Taahir Hassan,"IOT Based Power Theft Detection for Transmission Lines," 5th International Conference on Smart Electronics and Communication (ICOSEC 2024), IEEE, pp. 507–512, 2024.
[2] S. P. Daniel Chowdary, "Power theft detection system with RF communication between distribution and customer usage," in Proc. IEEE PES Conf., 2020, pp. 566–572.
[3] M. Saad, M. F. Tariq, A. Nawaz, and M. Y. Jamal, "Theft detection based GSM prepaid electricity system," in Proc. IEEE Int. Conf. Control Science and Systems Engineering (ICCSSE), 2017, pp. 435–438.
[4] G. A. Renuka, "Development of a cost-effective power theft detection and prevention system based on IoT Technology," in Proc. IEEE NIGERCON, 2019, pp. 756– 760.
[5] S. Visalatchi and K. K. Sandeep, "Smart energy metering and power theft control using Arduino & GSM," in 2nd Int. Conf. I2CT, 2020, pp. 858–961.
[6] T. Hasan, D. Q. U., and S. Zada, "Non-Technical Loss Detection, Prevention and Suppression issues for AMI in Smart Grid," 2018, pp. 217–288.
[7] M. Y. Jamel, "Prepaid electricity system using PIC microcontroller and GSM communication for secure energy management in Pakistan," *International Journal of Electrical and Electronics Engineering*, vol.